Cryptanalysis and Countermeasure of "An Efficient NTRU-based Authentication Protocol in IoT Environment"

YoHan Park[1], Woojin Seok[2], Wonhyuk Lee[3], Hong Taek Ju[4]
Department of Computer Engineering
Keimyung University, Korea, Republic[1,4]
KREONET Center, KISTI, Korea, Republic[2,3]

***Abstract*—A quantum computer is a paradigm of information processing that can show remarkable possibilities of exponentially improved information processing. However, this paradigm could disrupt the current cryptosystem, which is called quantum computing attacks, by calculating factoring problem and discrete logarithm problem. Recently, NTRU is applied to various security systems, because it provides security against to provide security against quantum computing attacks. Furthermore, NTRU provides similar security level and efficient computation time of encryption/decryption compared to traditional PKC. In 2018, Jeong et al. proposed an user authentication and key distribution scheme using NTRU. They claimed that their scheme provides various security properties and secure against quantum computing attacks. In this paper, we demonstrate that their scheme has security pitfalls and incorrectness in login and authentication phase. We also suggest countermeasures to fix the incorrectness and provide security against various attacks.**

Keywords*—*Post-quantum; NTRU; biometrics; user authentication; key agreement

I. Introduction

Development of Internet of Things (IoT) technology help users connect service providers easily and fast and utilize various services such as Health care, SmartHome, SmartGrid, and so on. However, IoT environments have threats to security and privacy because of its wireless nature [1]. Such threats hinder users make use of beneficial applications and service providers may not continue to invest for profits. Security problems should get solved to make the IoT-based services widely spread and applied.

User authentication and key agreement are essential requirement among all other security concerns. Those security services provide integrity and confidentiality for IoT environments [2]–[4]. Malicious adversaries will freely access user's critical and valuable information if secure authentication and key agreement methods do not provide.

Security of public key cryptosystem (PKC) are mostly based on the difficulty of factorization problem (FP) or discrete logarithm problem (DLP). RSA and elliptic curve cryptosystem (ECC) are major the examples of current cryptosystems based on FP and DLP. However, these algorithms are vulnerable to a quantum computing attack. In 1994, Peter W. Shor [5] proposed a quantum computing algorithm which can solve FP efficiently. And a quantum search algorithm proposed by Grover [6] can easily solve DLP. These algorithms based on quantum computing became major threats to all security protocols using RSA or DLP. Therefore, ETSI [7] and NIST [8] recommended that post-quantum cryptosystem (PQC) should be prepared with high priority.

There are several PQC which are secure against quantum computing attacks. These cryptosystems use Code, Lattice, Hash and Multivariate to provide security in quantum computing environments. Among many algorithms of PQC, NTRU, proposed by J. Hoffstein [9] in 1996, has been approved for standardization by Institute of Electrical and Electronics Engineerings (IEEE) [10]. The security of NTRU is based on the difficulty on a finding shortest path in n-th degree Lattice. Comparing to traditional PKC, NTRU provides not only similar security level, but also efficient computation time of encryption/decryption. Recently, NTRU is applied to various security systems which provides user authentication and key agreement.

Recently, a number of authentication and key agreement schemes have been proposed in IoT environments [11], [12], [19]. In 2017, Li et al. [13] proposed a key distribution protocol using ECC in IoT. However, the scheme is vulnerable to quantum computing attacks, such as Shor [5] or Grover [6] algorithm. To overcome these security pitfalls, Jeong et al. proposed an efficient NTRU-based authentication protocol in IoT environments [14] in 2018. They proposed user authentication and key agreement protocols using NTRU and claimed their scheme is secure against quantum computing attacks and prevents impersonations attack and session key disclosure attack. However, we find out that their scheme does not provide a proper user authentication process and is weak to various attacks, such as privileged insider attacks, impersonation attacks, and session key disclosure attacks. In addition, we show their scheme fails to provide correctness in login phase and authentication phase.

In this paper, we show the security weaknesses of Jeong et al.'s scheme. In addition, we propose countermeasures for the weaknesses of Jeong et al.'s scheme.

A. Contributions

The contributions made in the paper are listed below:

1) We demonstrate that Jeong et al.'s scheme has an incorrectness in login phase and authentication phase.
2) We analyze security weaknesses of Jeong et al.'s scheme and show that their scheme is vulnerable to privilege insider attacks, impersonation attacks, and session key disclosure attacks.
3) We propose countermeasures to overcome the security weaknesses of Jeong et al.'s scheme. The countermeasures help to prevent various attacks such as password guessing attacks, user impersonation attacks and session key disclosure attacks from malicious adversaries.

B. Paper Structure

The rest of the paper is organized as follows. In Section II, we introduce preliminaries used in this paper. In Section III, we review Jeong et al.'s scheme followed by the cryptanalysis of Jeong et al.'s scheme in Section IV. In Section V, we propose countermeasures for the weaknesses of Jeong et al.'s scheme. Finally, Section VI concludes the paper.

II. Preliminaries

A. NTRU

NTRU is a lattice-based public key cryptosystem proposed by Jeffry Hoffstein et al. [9]. This provides a similar security level, but high performance compared to RSA and ECC because of low computational complexity of polynomial convolution operation. NTRU requires $O(n^2)$ operations to encrypt or decrypt a message of size n, but RSA and ECC require $O(n^3)$ operations. NTRU, furthermore, resists quantum computing attacks and has adopted standard as IEEE 1363.1 and X9.98. NTRU cryptosystem consists of three parts: key generation, encryption and decryption.

1) Key generation: Alice and Bob are required to generate private/public key in advance to exchange data securely in PKC. The detail steps of key generation are as follows:

Step 1: Alice chooses two polynomials f and g with degree $N-1$ and coefficients in $\{-1, 0, 1\}$.

Step 2: The polynomial $f \in L_f$ must have the inverse element for modulo p and q. Alice computes $f * f_p^{-1} \equiv 1$ (mod p) and $f * f_q^{-1} \equiv 1$ (mod q).

Step 3: If f does not have an inverse element, Alice turns back to Step 1 and chooses another f. Otherwise, Alice computes the public key $h = pf_q^{-1} * g$ (mod q).

f and g are private keys and h is a public key of Alice.

2) Encryption: If Bob wants to send a message to Alice securely, Bob performs the encryption as follows:

Step 1: Bob who wants to send a plaintext polynomial $m \in L_m$ chooses a random polynomial $r \in L_r$ with $N-1$ degree and small coefficients. Coefficients are not restricted to the set $\{-1, 0, 1\}$.

Step 2: Bob encrypts the message m into e using the public key h of Alice. $e = r * h + m$

Step 3: Bob sends the encrypted message e to Alice.

3) Decryption: After receiving e from Bob, Alice decrypts the message as follows:

Step 1: Alice calculates a convolution $a = e * f$ (mod q), where f is a private key of Alice. The coefficient of a should satisfy $A \leq a_i \leq A + q$.

Step 2: Alice retrieves $m \equiv a$ (mod p).

B. Notations

Table I describe the notations used throughout the paper.

TABLE I. Notations

Notation	Meaning
U_A	user A
ID_A	identity of U_A
PW_A	password of U_A
RPW_A	pseudo password of U_A
B_A	biometric template of U_A
SC_A	smart card of user U_A
GWN	gateway node
$*$	convolution computation
f, g	private key polynomial $f \in L_f, g \in L_g$
f_p^{-1}, f_q^{-1}	inverse polynomial of f
h	public key
H	hash function
$\|\|$	concatenate operation
$\bigoplus$	XOR operation

III. Review of Jeong et al.'s Scheme

In this section, we review Jeong et al.'s NTRU-based authentication scheme. The scheme is composed of three phases: user registration phase, things registration phase, and login-authentication-key distribution phase.

A. User Registration Phase

In this phase, a user registers his/her information to the gateway node, and acquires a personalized smart card SC_A. The Jeong et al.'s user registration phase is illustrated in Fig. 1, and the detailed steps of this registration phase are as follows:

Step 1: A user U_A chooses ID_A and PW_A, then generates a random number x_A. Then, U_A selects polynomials $f_A \in L_f$ and $g_A \in L_g$, then calculates inverse elements f_{Ap}^{-1} and f_{Aq}^{-1} of f. Next U_A calculates the public key $h_A = pf_{Ap}^{-1} * g_A(modq)$ and the pseudo password $RPW_A = H(PW_A||x_A)$. U_A sends the registration request message $\{ID_A, RPW_A, h_A\}$ to the gateway node via a secure channel.

Step 2: After receiving registration request message from the user, the gateway node GWN stores the pair $\{ID_A, h_A\}$ in database. GWN also selects polynomials $f_B \in L_f$ and $g_B \in L_g$, then calculates inverse elements f_{Bp}^{-1} and f_{Bq}^{-1} of f. Next GWN calculates the public key $h_B = pf_{Bp}^{-1} * g_B(modq)$. Next, GWN computes $H(ID_A||RPW_A||h_A)$, and issues a smart card SC_A with $H(ID_A||RPW_A||h_A)$ and sends $\{SC_A, h_B\}$ to U_A.

Step 3: After receiving $\{SC_A, h_B\}$ from the GWN, U_A computes $V_A = H(ID_A||RPW_A||H(B_A))$, where B_A

User (U_A)		**Gateway Node** (GWN)
chooses ID_A and PW_A, generates x_A, selects $f_A \in L_F, g_A \in L_g$, calculate f_{Ap}^{-1}, f_{Aq}^{-1}, computes $h_A = f_{Ap}^{-1} * g_A$, $RPW_A = H(PW_A \vert\vert x_A)$		
	$\xrightarrow[\text{(secure channel)}]{\{ID_A, RPW_A, h_A\}}$	
		selects $f_B \in L_f, g_B \in L_g$, calculates f_{Bp}^{-1}, f_{Bq}^{-1}, computes $h_B = f_{Bp}^{-1}$, stores ID_A and h_A in the database, Generates $SC_A = H(ID_A \vert\vert RPW_A \vert\vert h_A)$
	$\xleftarrow[\text{(secure channel)}]{\{SC_A, h_B\}}$	
imprints biometrics B_A, computes $V_A = H(ID_A \vert\vert RPW_A \vert\vert H(B_A))$, store x_A and V_A into SC_A		

Fig. 1. User Registration Phase of Jeong et al.'s Scheme

is the biometric information of U_A. Then U_A stores V_A and x_A in SC_A.

B. Things Registration Phase

In this phase, a thing registers its information to the gateway node GWN, and receives an ephemeral key z_S from GWN. The Jeong et al.'s things registration phase is illustrated in Fig. 2, and the detailed steps of this registration phase are as follows:

Step 1: A thing chooses a random number n_S, then sends it to GWN through the secure channel.

Step 2: After receiving n_S from the thing, GWN choose a random number n_Z. Then GWN stores the pair (n_S, n_Z) in the database. Finally, GWN sends z_S to the thing via secure channel.

Step 3: After receiving n_Z from GWN, the thing stores n_Z in it's database.

C. Login-Authentication-Key Distribution Phase

In this phase, a user uses his/her multi-factor keys to login and authenticate oneself with GWN. Then a user shares session key SK with a thing. The Jeong et al.'s login-authentication-key distribution phase is illustrated in Fig. 3, and the detailed steps of this registration phase are as follows:

Step 1: A user inputs ID_A, PW_A, and imprints the biometrics B_A into the smart card SC_A. Then, SC_A computes RPW_A, V'_A, and verifies the validity of the user as follows:

$$\begin{aligned} RPW_A &= H(PW_A||x_A) \\ V'_A &= H(ID_A||RPW_A||H(B_A)) \\ \text{verifies } V'_A &\overset{?}{=} V_A \end{aligned}$$

If it is wrong, SC_A quits the login process. Otherwise, SC_A chooses random numbers r_A, k_A and computes I_A, e_A as follows:

$$\begin{aligned} I_A &= H(ID_A||RPW_A) \\ e_A &= pr_A * h_B + k_A \end{aligned}$$

Then, the user sends $\{I_A, e_A, h_A\}$ to GWN.

Step 2: After receiving $\{I_A, e_A, h_A\}$, GWN verifies I_A using the stored pair $\{ID_A, h_A\}$. Then, GWN retrieves k_A, and computes c_B as follows:

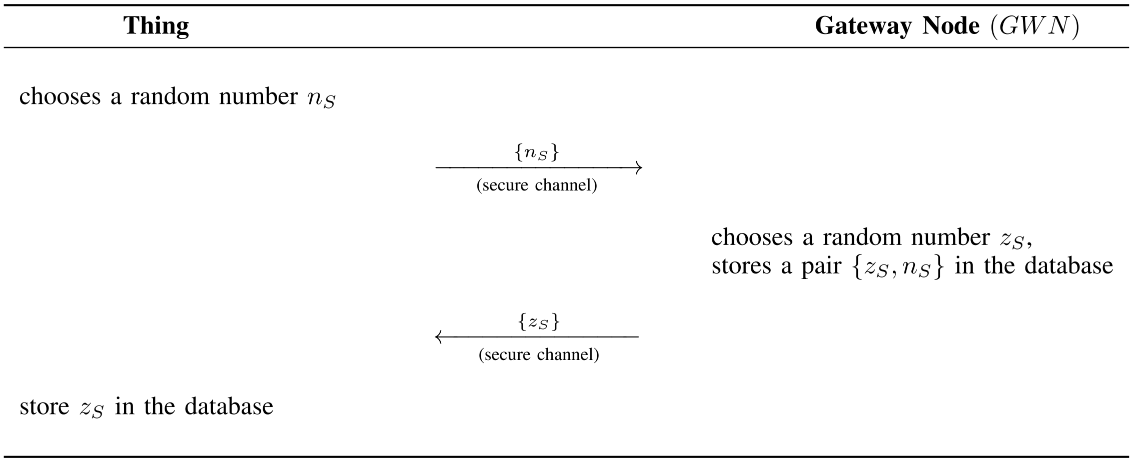
$$\begin{aligned} I_A &= H(ID_A||RPW_A) \\ a_B &= f_B * e_A (\text{mod } q) \\ k_A &= f_B^{-1} * a_A (\text{mod } p) \\ c_B &= z_S \oplus k_A \end{aligned}$$

Then, GWN sends c_B to the thing.

Step 3: After receiving c_B from GWN, the thing retrieves $k_A = c_B \oplus z_S$. Then the thing chooses a random number k_S and computes a session key $SK = H(k_A||k_S||n_S)$. The thing computes $c_S = k_S \oplus z_S$ and sends it to GWN.

Step 4: After receiving c_S, GWN chooses a random number $r_B \in L_r$ and computes k_S and e_B as follows:

$$\begin{aligned} k_S &= c_S \oplus z_S \\ e_B &= pr_B * h_A + (k_S||n_S) (\text{mod } q) \end{aligned}$$



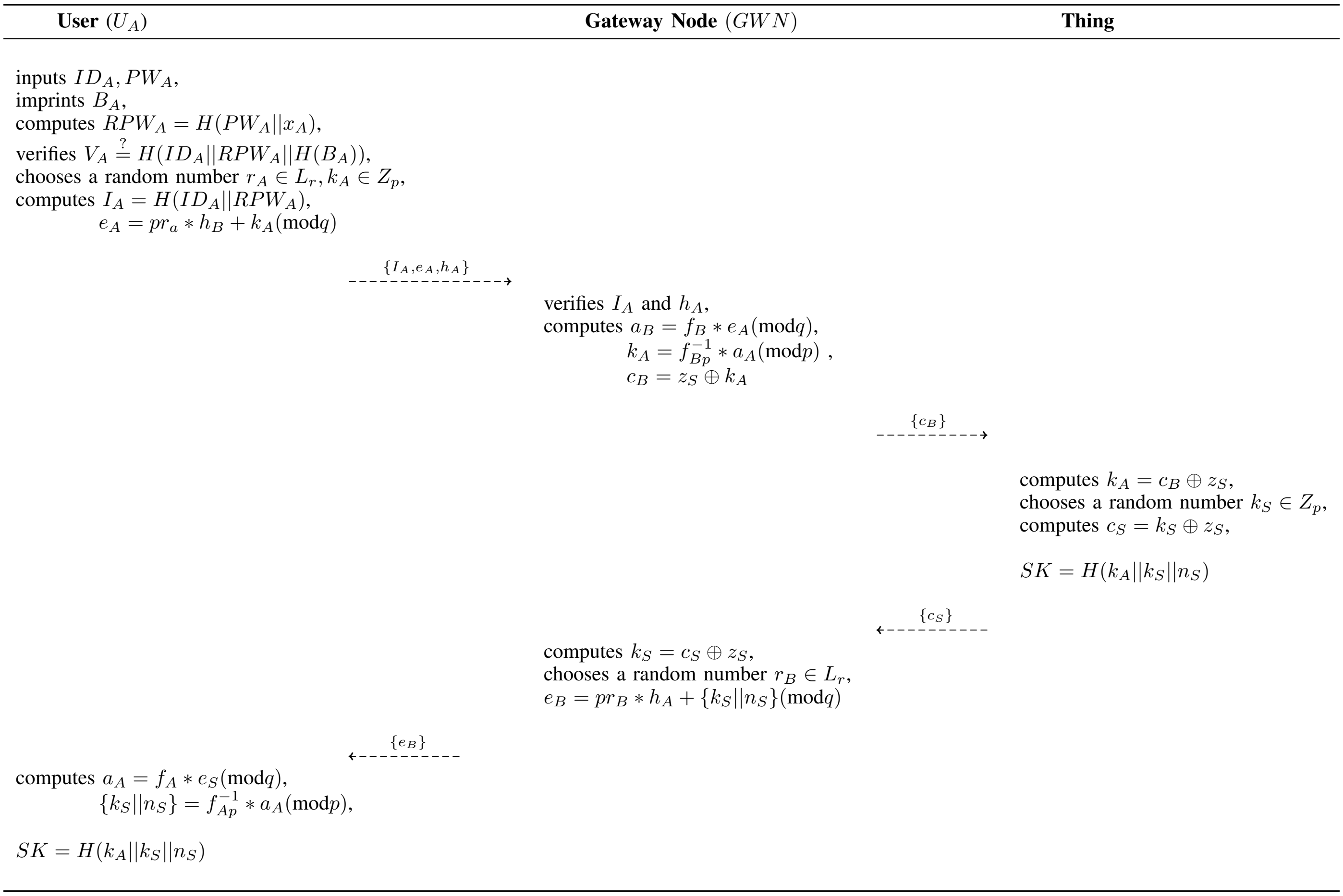
Thing | **Gateway Node** (GWN)

chooses a random number n_S

chooses a random number z_S,
stores a pair $\{z_S, n_S\}$ in the database

store z_S in the database

Fig. 2. Thing registration phase of Jeong et al.'s scheme



User (U_A) | **Gateway Node** (GWN) | **Thing**

inputs ID_A, PW_A,
imprints B_A,
computes $RPW_A = H(PW_A||x_A)$,
verifies $V_A \overset{?}{=} H(ID_A||RPW_A||H(B_A))$,
chooses a random number $r_A \in L_r, k_A \in Z_p$,
computes $I_A = H(ID_A||RPW_A)$,
$e_A = pr_a * h_B + k_A(\text{mod}q)$

verifies I_A and h_A,
computes $a_B = f_B * e_A(\text{mod}q)$,
$k_A = f_{Bp}^{-1} * a_A(\text{mod}p)$,
$c_B = z_S \oplus k_A$

computes $k_A = c_B \oplus z_S$,
chooses a random number $k_S \in Z_p$,
computes $c_S = k_S \oplus z_S$,

$SK = H(k_A||k_S||n_S)$

computes $k_S = c_S \oplus z_S$,
chooses a random number $r_B \in L_r$,
$e_B = pr_B * h_A + \{k_S||n_S\}(\text{mod}q)$

computes $a_A = f_A * e_S(\text{mod}q)$,
$\{k_S||n_S\} = f_{Ap}^{-1} * a_A(\text{mod}p)$,

$SK = H(k_A||k_S||n_S)$

Fig. 3. Login-Authentication-Key Distribution Phase of Jeong et al.'s Scheme

Then, GWN sends e_B to the user.

Step 5: After receiving e_B, the user computes $k_S||n_S$ and the session key SK as follows:

$$\begin{aligned} a_A &= f_A * e_B \\ k_S||n_S &= f_{AP}^{-1} * a_A \\ SK &= H(k_A||k_S||n_S) \end{aligned}$$

IV. Cryptanalysis of Jeong et al.'s Scheme

In this section, we demonstrate the security flaws of Jeong et al.'s scheme. Their scheme does not provide correctness at the login phase and the key distribution phase. Thus, the user who tries to connect a IoT device cannot login to GWN and share a session key. In addition, the scheme is vulnerable to privileged insider attacks. The insider adversaries can sneak into the database of GWN and illegally capture the stored information. The adversaries can guess identity and password of users using the captured information and impersonate a legitimate user.

In this paper, we assumed that an adversary $\mathcal{A}$ could steal or obtain the user's smart card SC_A. In addition, an adversary $\mathcal{A}$ could extract information $\{H(ID_A||RPW_A||h_A), V_A, x_A\}$ from the smart card [15] and could get previous session messages transmitted through public network. The description of the security weaknesses of Jeong et al.'s scheme is as follows.

A. Incorrectness

1) Incorrectness at the login phase: In the login phase, GWN verifies the validity of a user by comparing the received value I_A with the computed value $H(ID_A||RPW_A)$. If it is correct, GWN authenticates the user and proceeds the key distribution phase. GWN can find ID_A using the pair $\{ID_A, h_A\}$ stored in the database. However, GWN cannot get RPW_A in the database and other transmitted values. Therefore, GWN cannot check the legitimacy of a user who wants to access things.

2) Incorrectness at the key distribution phase: To establish a session key between a user and a thing, each party should know the information $\{k_A, k_S, n_S\}$. k_A is a random number generated by a user, and encrypted with the pubic key h_B of GWN. To retrieve k_A from the encrypted message e_A, Jeong et al.'s present the mathematical equation as follows:

$$\begin{aligned} a_B &= f_B * e_A (\text{mod } q) \\ k_A &= f_B^{-1} * a_A (\text{mod } p) \end{aligned}$$

Unfortunately, it is incorrect and cannot find k_A. The equation should be presented as follows:

$$\begin{aligned} a_B &= e_A * f_B (\text{mod } q) \\ &= (pr_A * h_B + k_A) * f_B (\text{mod } q) \\ &= (pr_A * h_B * f_B) + (k_A * f_B)(\text{mod } q) \\ &= k_A * f_B (\text{mod } q) \\ a_B * f_B^{-1} (\text{mod } p) &= k_A * f_B * f_B^{-1} (\text{mod } p) \\ &= k_A (\text{mod } q) \end{aligned}$$

In addition, a user cannot retrieve $\{k_S||n_S\}$ from a_A, because GWN sends e_B but a user decrypt e_S. e_S should be replaced with e_B.

B. Privileged Insider Attack

Jeong et al.'s analyzed their scheme and insisted that the scheme is secure against privileged insider attacks. However, we cryptanalyze and show that their scheme is vulnerable to the attacks. A malicious inside adversary can access to the database and compute user's information, then guess identities of users. Using the information, the adversary can act as a legal user as follows:

1) An insider adversary $\mathcal{A}$ can get the values $\{ID_A, h_A\}$ stored in the database and $\{H(ID_A||RPW_A||h_A), V_A, x_A\}$ from the smart card SC_A.
2) $\mathcal{A}$ performs an offline password guessing attack. $\mathcal{A}$ guesses a password PW'_A and computes $RPW'_A = H(PW'_A||x_A)$.
3) $\mathcal{A}$ compares the computed value $H(ID_A||RPW'_A||h_A)$ with $H(ID_A||RPW_A||h_A)$ which is stored in SC_A. If it matches, $\mathcal{A}$ successfully guesses the password of the user.

Therefore, Jeong et al.'s scheme does not provide security against privileged insider attacks.

C. Impersonation Attack

Jeong et al. claimed that their scheme is secure against impersonation attacks. However, once the inside adversary $\mathcal{A}$ correctly guesses PW_A and finds secret values, such as ID_A and RPW_A, $\mathcal{A}$ can generate the login message $\{I_A, e_a, h_A\}$. Then, $\mathcal{A}$ can impersonate the user.

D. Session Key Disclosure Attack

Jeong et al.'s insisted that the scheme provides session key disclosure attacks. But, we show that their scheme is weak to this attack. An inside adversary can access to the database and obtain secret information pair of Things $\{n_S, z_S\}$. The adversary can compute a session key using the information as follows:

1) The insider adversary $\mathcal{A}$ who knows $\{n_S, z_S\}$ can acquire c_B and c_S which are transferred via a insecure channel.
2) $\mathcal{A}$ can compute $k_A = c_B \oplus z_S, k_S = c_S \oplus z_S$, because $\mathcal{A}$ knows z_S from the database and c_B and c_S from an insecure channel.
3) $\mathcal{A}$ who successfully computes k_A and k_S can finally derive a session key $SK = H(k_A||k_S||n_S)$, because n_S is also disclosed.

Therefore, Jeong et al.'s scheme is vulnerable to session key disclosure attacks.

V. Countermeasures

In this section, we present the fixes for the incorrectness and the countermeasures to improve the security weakness of Jeong et al.'s scheme.

A. Fixes for the Incorrectness

Jeong et al.'s scheme cannot provide the user authentication, because GWN cannot computes I_A using the data in the database. GWN should know the pair $\{ID_A, RPW_A\}$ to compute I_A and verify the validity of user U_A. Therefore, GWN should store the three sets $\{ID_A, RPW_A, h_A\}$ in the database at the user registration phase.

Unfortunately, if GWN store that tuple in the database, privileged insider can easily obtain ID_A and RPW_A, and compute I_A without password guessing process. To solve this problem, I recommend not to allow storing the identity and password of a user in the database. Instead, a user generates a pseudo-identity and sends it to GWN for the verification. There are many authentication schemes which do not allow to store the identity of a user but provide an authentication of a user [16]–[18].

The fixes for the incorrectness at the key distribution phase are introduced at Section IV.

B. Countermeasure of Privileged Insider Attacks

The privileged insider adversary $\mathcal{A}$ can use the data ID_A stored in the database. $\mathcal{A}$ uses this identity and the data $H(ID_A||RPW_A||h_A)$ stored in the smart card. Unfortunately, $H(ID_A||RPW_A||h_A)$ is not utilized along Jeong et al.'s scheme, i.e. it is useless data. Therefore, GWN does not need to store the data when it generates a smart card. If that data is not in the smart card, $\mathcal{A}$ cannot correctly guess PW_A and RPW_A. Then the scheme provide security against privileged insider attacks.

C. Countermeasure of Impersonation Attacks

The adversary $\mathcal{A}$ can impersonate the user, because $\mathcal{A}$ can computes I_A. However, we mentioned, just before, that the scheme could provide security against privileged insider attacks and $\mathcal{A}$ cannot guess PW_A and RPW_A. Therefore, $\mathcal{A}$ cannot computes I_A as well.

D. Countermeasure of Session Key Disclosure Attacks

The session key is easily disclosed, because the random numbers k_A and k_S are encrypted with same key z_S. To prevent this attack, the random number should be encrypted with other data [19], [20] or another method to conceal data [21]

VI. Conclusions

User authentication and key agreement are important security requirements for IoT environments. And several multi-factor authentication schemes have been proposed in recent years. However, these schemes are vulnerable to quantum computing attacks and the security threats should be resolved. Recently, Jeong et al.'s proposed a NTRU-based user authentication scheme in IoT environments. They insisted that their scheme provides various security properties, even security against the quantum computing attacks. Unfortunately, we found out that their scheme has some incorrectness in authentication phase and security weakness against the privileged insider adversary. We presented the fixes for the incorrectness and the countermeasure for the security weakness. The scheme with the countermeasures provides a proper user authentication and security properties against various attacks.

For further works, we are designing completely a security-enhanced NTRU-based user authentication scheme in IoT environments.

Acknowledgment

This research was sponsored by 'QKD based next generation KREONET project' of KISTI.

References

[1] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E. J. Yoon, and K. Y. Yoo, *"Secure signature-based authenticated key establishment scheme for future IoT applications"*, IEEE Access, 5, 3028-3043, 2017.

[2] M. Turkanovic, B. Brumen, and M. Hölbl, A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion, Ad Hoc Networks 20, pp. 96-112, 2014.

[3] X. Yao, X. Han, X. Du, and X. Zhou, A lightweight multicast authentication mechanism for small scale IoT applications, IEEE Sensors Jour., 13(10), pp. 3693-3701, Oct., 2013.

[4] B. Ndibanje, H. J. Lee, and S. G. Lee, Security analysis and improvements of authentication and access control in the internet of Things, Sensors, 14(8), pp. 14786-14805, 2014.

[5] P. W. Shor, *"Algorithms for Quantum Computation : Discrete Logarithms and Factoring"*, Proceedings of 35th Annual Symposium on Foundations of Computer Science and IEEE Computer Society, 124-134, 1994.

[6] L. K. Grover, *"A Fast Quantum Mechanical Algorithm for Database Search"*, STOC 96' Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing, 212-219, 1996.

[7] ETSI, Quantum Safe Cryptography and Security, ISBN No. 979-10-92620-09-0, 2015.

[8] NIST, Report on Post-Quantum Cryptography, IR 8105, 2016.

[9] J. Hoffstein, J. Pipher, and J. H. Silverman, *"NTRU: A Ring-Based Public Key Cryptosytem"*, Algorithmic Number Theory, ANTS 1997, Lecture Notes in Computer Science (LNCS), Vol. 1423, 278-288, 1998.

[10] IEEE, *IEEE P1363.1 Draft 10: Draft Standard for Public Key Cryptographic Techniques Based on Hard Problems over Lattices, International Association for Cryptologic Research Eprint archive, 2008.*

[11] S. Roy, S. Chatterjee, and G. Mahapatra, *"An efficient biometric based remote user authentication scheme for secure internet of things environment",* Journal of Intelligent & Fuzzy Systems, 34(3), 1403-1410, 2018.

[12] K. S. Park, S. K. Noh, H. J. Lee, A. K. Das, M. H. Kim, and Y. H. Park, *"LAKS-NVT: Provably Secure and Lightweight Authentication and Key Agreement Scheme without Verification Table in Medical Internet of Things"*, IEEE Access, 8, 119387-119404, 2020.

[13] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo, *"A Three-Factor Anonymous Authentication Scheme for Wireless Sensor Networks in Internet of Things Environments*, Journal of Network and Computer Applications 103, 194-204, 2018.

[14] S. H. Jeong, K. S. Park, Y. H. Park, and Y. H. Park, *"An Efficient NTRU-Based Authentication Protocol in IoT Environment"*, Intelligent Computing, SAI 2018, Advances in Intelligent Systems and Computing, vol 857. Springer, 1262-1268, 2019.

[15] P. Kocher, J. Jaffe, and B. Jun, *"Differential power analysis",* in Proc. 19th Annu. Int. Cryptol. Conf., Santa Barbara, CA, USA, Aug. 1999.

[16] S. J. Yu, J. Y. Lee, Y. H. Park, Y. H. Park, S. W. Lee, and B. H Chung, *"A Secure and Efficient Three-Factor Authentication Protocol in Global Mobility Networks"*, Applied Sciences 10, no. 10, 2020.

[17] S. J. Yu, K. S. Park, Y. H. Park, H. P. Kim, and Y. H Park, *"A Lightweight Three-Factor Authentication Protocol for Digital Rights Management System"*, Peer-to-Peer Networking and Applications, 2020.

[18] K. S. Park, Y. H. Park, A. K. Das, S. J. Yu, J. Y. Lee, and Y. H Park, *"A Dynamic Privacy-Preserving Key Management Protocol for V2G in Social Internet of Things"*, IEEE Access, 7, 2019.

[19] H. J. Lee, D. W. Kang, J. H. Ryu, D. H. Won, H. S. Kim, and Y. S. Lee, *"A Three-Factor Anonymous User Authentication Scheme for Internet of Things Environments"*, Journal of Information Security and Applications, 52, 2020.

[20] S. Ahmed, S. Kumari. M. A. Saleem, K. Agarwal, K. Mahmood, and M. H. Yang, *"Anonymous Key-Agreement Protocol for V2G Environment Within Social Internet of Vehicles"*, IEEE Access, 8, 2020.

[21] K. S. Park, S. K. Noh, H. J. Lee, A. K. Das, M. H. Kim, Y. H. Park, and M. Wazid, *LAKS-NVT: Provably Secure and Lightweight Authentication and Key Agreement Scheme Without Verification Table in Medical Internet of Things*, IEEE Access, 8, 2020.